Lecture 19: Cyclotomic Fields and Applications

$\mathbb{Q}(\zeta_n)$ with $\zeta_n = e^{2\pi i/n}$; $\mu_n = \{z \in \mathbb{C} \mid z^n = 1\}$

$\Phi_n(x) = \prod_{\substack{\zeta \in \mu_n \\ \text{primitive}}} (x - \zeta)$. Then $x^n - 1 = \prod_{d|n} \Phi_d(x)$

Thm: For any n, $\Phi_n(x)$ is in $\mathbb{Z}[x]$ and is irreducible.

Hence $[\mathbb{Q}(\zeta_n):\mathbb{Q}] = |\mu_n^{\text{Primitive}}| = \phi(n)$.

Pf that $\Phi_n(x) \in \mathbb{Z}[x]$: We induct on n.

Set $f(x) = \prod_{\substack{d|n \\ d<n}} \Phi_d(x)$, so then $x^n - 1 = f(x)\Phi_n(x)$

in $\mathbb{Q}[x]$ by induction

In $\mathbb{Q}[x]$ have $x^n - 1 = q(x)f(x) + r(x)$ with

$\deg r < \deg f$. Then in $\mathbb{C}[x]$ have

$$\Phi_n(x)f(x) = q(x)f(x) + r(x) \Rightarrow \big(\Phi_n(x) - q(x)\big)f(x) = r(x)$$

$\Rightarrow r(x) = 0$ as $\deg r < \deg f$. So $\Phi_n(x) = q(x)$

and $\Phi_n(x) \in \mathbb{Q}[x]$ and by Gauss in $\mathbb{Z}[x]$ as well.

<u>Proof of Irreducibility</u>: Suppose $\Phi_n = f \cdot g$ for $f, g \in \mathbb{Z}[x]$ with f irreducible.

<u>Claim</u>: Suppose ζ is a root of f. If p is a prime not dividing n, then ζ^p is also a root of f.

Assuming this, let ζ be a fixed root of f. Then any primitive n^{th} root is ζ^m where $m = p_1 p_2 \cdots p_k$ and all $p_i \nmid n$. As $\zeta^m = (((\zeta^{p_1})^{p_2})^{p_3} \cdots)^{p_k}$ repeatedly applying the claim gives ζ^m is a root of f. So $f(x) = \Phi_n(x)$ and so $\Phi_n(x)$ is irred.

<u>Proof of Claim</u>: Suppose instead $g(\zeta^p) = 0$. Thus ζ is a root of $g(x^p) \Rightarrow g(x^p) = f(x) \cdot h(x)$ for some $h(x) \in \mathbb{Z}[x]$. Let's look in $\mathbb{F}_p[x]$:

① $x^n - 1$ is separable as $nx^{n-1} \neq 0$ in $\mathbb{F}_p[x]$.
So $\overline{\Phi}_n(x)$ has distinct roots.

② The Frobenius map $\mathbb{F}_p \to \mathbb{F}_p$ is the identity, since $a^p = a$ for all $a \in \mathbb{F}_p$ as discussed last time. Hence $\bar{g}(x^p) = (\bar{g}(x))^p$ for all $\bar{g} \in \mathbb{F}_p[x]$.

③ As $\bar{g}(x)^p = \bar{f}(x)\bar{h}(x)$, we see $\bar{g}$ and $\bar{h}$ have a common root.

But then by ③ the poly $\bar{\Phi}_n = \bar{g}\bar{f}$ has a multiple root, a contradiction. $\blacksquare$

<u>Thm</u>: $m \in \mathbb{Z}_{>0}$. There are infinitely many primes $p \equiv 1 \bmod m$, i.e. $p = cm + 1$.

[Special case of Dirichlet's Thm on Primes in Arithmetic Progressions.]

<u>Proof</u>: Consider $\Phi_m(a)$ for $a \in \mathbb{Z}_{>0}$. Then

① There are infinitely many primes which divide some $\Phi_m(a)$.

② Any $p \mid \Phi_m(a)$ with $p \nmid m$ has $p \equiv 1 \bmod m$.

① is true for all monic polys in $\mathbb{Z}[x]$, so will focus on ②.

In $\mathbb{F}_p$, have $a^m - 1 = \Phi_m(a) \cdot \prod_{\substack{d|m \\ d<m}} \Phi_d(a) = 0$

<u>Claim</u>: a has order m in $\mathbb{F}_p^\times$.

<u>Pf of Claim</u>: Suppose $a^d = 1$ for $d < m$. Now $d | m$ and so a is a root of some $\Phi_{d'}$ for $d' | d$. But then $x^m - 1$ has a multiple root, a contradiction as $m x^{m-1} \neq 0$ in $\mathbb{F}_p[x]$. So a has order m in $\mathbb{F}_p^\times$.

<u>Pf of ②</u>: As a has order m, we have $m \mid |\mathbb{F}_p^\times| = p-1$

$\Rightarrow p = cm+1$, as needed. $\square$

<u>Pf of ①</u>: More gen, let $f(x) \in \mathbb{Z}[x]$ be monic. Suppose $\{f(a) \mid a \in \mathbb{N}\}$ have only finitely many prime divisors $p_1, \ldots, p_k$. Choose a so that $f(a) = c \neq 0$.

Consider

$$g(x) = c^{-1} f(a + c\overbrace{p_1 \cdots p_k x}^{y}) \qquad n = \deg f$$

$$= c^{-1}\left(f(a) + f'(a)cy + \frac{f''(a)}{2}c^2y^2 + \cdots + \frac{f^{(n)}(a)}{n!}c^ny^n \right)$$

$$= 1 + f'(a)y + \frac{f''(a)}{2}cy^2 + \cdots + \underbrace{\frac{f^{(n)}(a)}{n!}}_{\text{in } \mathbb{Z}} c^{n-1}y^n$$

which is in $\mathbb{Z}[x]$.

For any b, have $g(b) \equiv 1 \bmod p_1 \cdots p_k$.

Pick b large enough so that $|g(b)| > 1$.

Let p be any prime factor of $g(b)$.

Then $p \neq p_i$ for all i and $p \mid f(a + cp_1 \cdots p_k b)$. ∎